



MEMORANDUM OF UNDERSTANDING and DATA SHARING AGREEMENT

This Memorandum of Understanding and Data Sharing Agreement ("MOU") is entered into on August 8, 2017 by and between Eckerd Youth Alternatives, Inc. d/b/a Eckerd Kids ("Eckerd Kids"), a Florida nonprofit corporation, Mindshare Consulting Group, LLC ("Mindshare") a Florida not-for-profit organization, and the New Hampshire Department of Health and Human Services, Division for Children, Youth and Families ("DCYF") with respect to the implementation and use of Eckerd Rapid Safety Feedback®. Eckerd Kids and Mindshare are sometimes referred to herein collectively as the "Providers". Eckerd Kids, Mindshare and DCYF are sometimes referred to herein collectively as the "Parties."

1. **Intent.** This MOU identifies the Parties' understandings of their rights and obligations to each other with respect to 1) the access to and sharing of DCYF Agency data and 2) the implementation and use of Eckerd Rapid Safety Feedback®.
2. **Purpose of Agreement.** Providers represent that the data specified in this MOU will be used solely for purposes of Eckerd Kids Rapid Safety Feedback®.
3. **Definitions:**
 1. *Agency* means the New Hampshire Department of Health and Human Services, Division for Children, Youth and Families ("DCYF").
 2. *Confidential Information* means information each party may come into contact with concerning the other party, including without limitation client records and other proprietary information which must remain confidential pursuant to the terms of this MOU.
 3. *Eckerd Rapid Safety Feedback®* means a program developed by Eckerd Kids that utilizes predictive analytics to help identify child welfare cases of the highest probability of a serious injury or death and identifying critical case practices, that when performed by the Agency to applicable standards, will greatly assist in keeping the child safe.
 4. *Eckerd Rapid Safety Feedback® Community of Practice* means the Agency participating in quarterly fidelity reviews and sharing information and reports with Eckerd Kids.
 5. *Fidelity Reviews* means a review by Providers to ensure the Agency is implementing Eckerd Rapid Safety Feedback® according to established practices.
 6. *CCWIS/SACWIS* means the jurisdiction's statewide automated child welfare information system referred to as Bridges.
 7. *Portal* means a website and related technology that is designed to read CCWIS/SACWIS information, perform automated analysis, and generate reports that can be used to implement and support Eckerd Rapid Safety Feedback®.

8. *Portal Terms* means the website usage terms available on the Portal that sets forth the terms and conditions under which the Agency may use the Portal. An example of the current portal terms and conditions are included here as Exhibit A. Exhibit A is NOT incorporated herein, but provided for information, only. The ruling website usage terms are those that are required to be accepted by the User at the time of Portal use.
9. *QA* means Agency Quality Assurance staff member that does not carry a caseload.

4. Introduction

1. Eckerd Kids is a not for profit corporation that specializes in human services, specifically child welfare. During the course of its business, Eckerd Kids has developed Eckerd Rapid Safety Feedback®, a program that has been successful in reducing the occurrence of serious injury or death in high risk dependency cases.
2. Eckerd Kids, and its affiliate, Mindshare operate using the Portal and related training materials to assist agencies that desire to implement Eckerd Kids Rapid Safety Feedback®.
3. Agency has chosen Eckerd Kids and its affiliate Mindshare to implement Eckerd Rapid Safety Feedback® in the State of New Hampshire and this MOU describes the responsibilities of the Providers and the Agency in connection with that implementation.

5. Eckerd Kid's Responsibilities

1. Eckerd Kids, with its affiliate, Mindshare, host, maintain and support the Web Portal with a goal of providing the Agency with 24 hour technical support and access to the Portal and the reports it generates. At no time will any Web Portal content or data be backed up, stored or hosted in any location outside of the United States. All data, associated in any way with the Web Portal will be owned solely by the Agency. Mindshare will not authorize or provide access credentials to any person other than Agency or Eckerd Kids employees who have a need for such access or credentials, without Agency's prior written consent. Mindshare will not provide administrative level access to the Web Portal or any database or data storage system used by the Web Portal to any person without Agency's prior written consent. Each employee of Mindshare who has access to the Web Portal or any database or data storage system used by the Web Portal will execute a confidentiality agreement reasonably acceptable to the Agency confirming the employee's duty to maintain all data and information relating to cases referenced in the Web Portal strictly confidential. Eckerd Kids and Mindshare will adhere to the "DHHS Information Security Requirements" which are attached to this agreement as Exhibit B and incorporated herein by reference.
2. Eckerd Kids, with its affiliate, Mindshare, will:
 - a. Adapt the Portal to create reports that provide a customized predictive data sample of prioritized cases for review;

- b. Provide training on review completion, portal entry, staffing techniques, and action item tracking to support the Agency's implementation of Eckerd Rapid Safety Feedback®;
- c. Provide Agency personnel with access to the Eckerd Rapid Safety Feedback® practice guide for use in connection with the Agency's implementation and offer same day technical assistance from case review staff experienced in the review process;
- d. Perform quarterly fidelity reviews and coordinate sharing of best practices across jurisdictions through the Eckerd Rapid Safety Feedback® Community of Practice; and,
- e. Provide additional reports as mutually agreed upon by Eckerd Kids and the Agency.

6. Agency's Responsibilities

- 1. The Agency will allow the Providers to access an extract of the Agency's CCWIS/SACWIS system on a daily basis. The agency will provide access to the client files of clients that died due to maltreatment and/or clients that experienced serious maltreatment while known to DCYF.
- 2. The Agency will:
 - a. Work with Mindshare to establish an agreed exchange protocol and accommodate the DCYF data exchange method and data packaging formats. The exchange protocol will include the specifications for the initial historical data package. A minimum of three years client data history should be provided within thirty days of signing the MOU;
 - b. Provide sufficient reviewers to the Eckerd Rapid Safety Feedback® program. Reviewers should be dedicated QA staff that are NOT investigating or managing the case or providing supervision to the front line workers assigned to the case. Reviewers must successfully complete Eckerd Rapid Safety Feedback® training (provided at no cost to the Agency) prior to completing case reviews;
 - c. Participate in a quarterly Fidelity Review, sharing lessons learned with other jurisdictions, and report the results observed after implementation of Eckerd Rapid Safety Feedback®;
 - d. Enter all case reviews into the Eckerd Rapid Safety Feedback® portal to provide automated tracking functionality, dashboards, and data for the continuous improvement of existing predictive data sets for the Eckerd Rapid Safety Feedback® implementation in New Hampshire; and,
 - e. Provide Providers written notice of any lawsuit or claim filed or asserted against the Agency alleging liability in connection with Eckerd Rapid Safety Feedback®

7. Term of MOU

- 1. This MOU will be effective upon execution by the parties and will terminate on December 31, 2018 (the "Term") unless terminated earlier pursuant to Section 7.2 below.

2. Any party may terminate this MOU for any reason with ten (10) calendar day written notice to the other parties.
3. There are no renewals to this MOU. The Parties may, however, negotiate a contract to continue Eckerd Rapid Safety Feedback® as mutually agreed upon.
4. If mutually agreed to by the Parties, this MOU may be extended for up to six (6) months to accommodate the negotiation of a contract to continue ERSF®.

8. Compensation

Compensation for Eckerd and Mindshare's services under this agreement will be provided by Casey Family Programs pursuant to an agreement between Casey Family Programs and the Department of Health and Human Services, Division for Children Youth and Families dated May 30, 2017, the terms of which are incorporated herein by reference.

9. Intellectual Property

1. All CCWIS/SACWIS data will be deemed and treated as Confidential Information of the Agency. All intellectual property rights in and to the CCWIS/SACWIS data will remain the sole property of the Agency. By making CCWIS/SACWIS data available to Providers, the Agency will grant, and hereby does grant, to Providers a limited, non-exclusive, royalty-free, fully-paid-up license for the term of this MOU to use the CCWIS/SACWIS data, but solely for the purpose of implementing Eckerd Rapid Safety Feedback® for the Agency, providing the Portal and related reports, and improving Eckerd Rapid Safety Feedback®.
2. All intellectual property rights in and to Eckerd Kids Rapid Safety Feedback®, the Portal and its related software and documentation, the reports generated by the Portal, the Eckerd Kids Rapid Safety Feedback® training materials, the Eckerd Kids Rapid Safety Feedback® safety guide (including without limitation for all of the foregoing, all related inventions, processes, improvements, trade secrets, algorithms, works of authorship, trademarks and service marks (jointly "Pre-existing IP")) is and will remain the sole property of the original owner (Eckerd Kids, its affiliate, Mindshare, and their licensors). All pre-existing IP will be deemed and treated as Confidential Information. Eckerd Kids and Mindshare will grant, and hereby does grant to the Agency, a limited, non-exclusive, royalty-free, fully-paid-up license for the term of this MOU to use their pre-existing IP, but solely for the purpose of implementing Eckerd Kids Rapid Safety Feedback® for the Agency and subject to this MOU and the Portal Terms.
3. By using the Portal, Agency is agreeing to abide by, and to be bound by, the Portal Terms and any applicable laws (including, without limitation laws relating to privacy and personal identifying information relating to children).

10. Background checks and verification

At the sole discretion of the Agency, Providers may be subject to user background checks, depending on the information systems Providers accesses

or types of data Agency provides. Providers must submit the required background check information to the agency in a timely manner, if requested.

11. HIPAA

Providers agree to use and disclose Protected Health Information in compliance with the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) (45 C.F.R. Parts 160 and 164) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and in accordance with the Business Associates Agreement which has been executed by the parties, is attached to this agreement as Exhibit C and incorporated herein by reference. The definitions set forth in the Privacy Rule (45 C.F.R. 160.103 and 164.501) are incorporated by reference into this agreement.

12. Governing Law, Venue, and Jurisdiction

This MOU will be governed by and construed in accordance with the laws of the State of New Hampshire, excluding any conflicts of laws, rule, or principle that might refer the governance or construction of this MOU to the law of another jurisdiction. The Parties agree that all disputes, claims, actions, or lawsuits between them, arising out of or relating to this MOU, or for alleged breach of this MOU, will be heard and determined by a Superior Court of the State of New Hampshire, or by any appellate courts which review decisions of those courts.

13. Entire Agreement

This MOU constitutes the entire agreement of the Parties with respect to the subject matter hereof, and supersedes any and all other agreements, understandings, negotiations, or representations between the Parties with respect thereto.

14. Confidentiality

Each Party agrees to maintain in confidence any information disclosed to it by, or discovered by it regarding, any other Party or Parties it knows or has reason to know is proprietary and/or confidential, including, without limitation, the terms of this MOU ("Confidential Information"). If the receiving Party becomes legally required to disclose Confidential Information, or any part thereof, the receiving Party shall give the disclosing Party prompt notice of such requirement. If the disclosing Party waives compliance with any of the terms of this Agreement or is unable to obtain a protective order or other appropriate remedy with respect to such disclosure of Confidential Information, then the receiving Party will disclose only that portion of the Confidential Information necessary to ensure compliance with such legal requirement. This Section shall survive termination of this MOU.

[SIGNATURE PAGE FOLLOWS]

- e. Severability. If any term or condition of this Exhibit I or the application thereof to any person(s) or circumstance is held invalid, such invalidity shall not affect other terms or conditions which can be given effect without the invalid term or condition; to this end the terms and conditions of this Exhibit I are declared severable.
- f. Survival. Provisions in this Exhibit regarding the use and disclosure of PHI, return or destruction of PHI and extensions of the protections of this Exhibit in section (3)(i), shall survive the termination of the Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Exhibit

Department of Health and Human Services

Eckerd Youth Alternatives, Inc. d/b/a Eckerd Kids ("Eckerd Kids")


Signature of Authorized Representative


Signature of Authorized Representative

Interim Director, DCYF
Title of Authorized Representative

Mindshare Consulting Group, LLC
("Mindshare")


Signature of Authorized Representative

8/11/2017
Date

8-8-17
Date

IN WITNESS WHEREOF, the Parties agree to the expressed terms.

Eckerd Youth Alternatives, Inc.

New Hampshire Division for Children, Youth and
Families (DCYF)

By: Nicole Stroebel

Name: Nicole Stroebel

Title: Controller

By: Christine Tappan

Name: Christine Tappan

Title: Interim Director, DCYF

Mindshare Consulting Group, LLC

By: Gregory Povolny

Name: Gregory Povolny

Title: Chief Executive Officer

Exhibit A: (Sample for info only)
Client Portal Terms and Conditions

The following constitutes the terms and conditions under which Mindshare Consulting Group, LLC, d/b/a Mindshare Technology, ('Mindshare') offers the information, services and facilities of Mindshare. Please read the terms and conditions carefully, if you do not agree to any of the terms and conditions you must not use the site.

Client Portal Eligibility & Use

The Mindshare Portal is only available to Mindshare clients or clients authorized to use the portal by a Mindshare authorized provider. To become a user of and have access to the Portal, Mindshare requires that you register and provide Mindshare with accurate user information.

Acceptable and Lawful Use of Site by Authorized Users

All users represent and attest that the information they provided when registering as a user, and all information that they subsequently provide regarding themselves is true and accurate and not misleading.

Use of Site

You may not use any robot, spider or other automated means to access the Site or content or services provided on the Site for any purposes. You may not use any means to index the Site in a search engine. You may not post content on the Site that contains any viruses or other computer programming routines that are intended to damage or detrimentally interfere with any system, data or personal information. You shall not attempt to make the Site unavailable through denial-of-service attacks or similar means.

User Notifications

If you register as a user, you agree that Mindshare may send information, warning and alert notices, and other messages per your preferences, to you via e-mail at the e-mail address you provide when registering to become a user (or which you later update).

User Password and Login Identity

You are responsible for maintaining the confidentiality of your user password, and user name/login, and are fully responsible for all activities that occur under your profile/account with or without your knowledge. If you knowingly provide your user name and password information to another person, your user privileges may be suspended temporarily or terminated. You agree to immediately notify Mindshare of any unauthorized use of your user password, user name or any other breach of security.

Ownership and Intellectual Property

Other than content provided by the jurisdiction which includes the content presented in the dashboards, and other than supplemental review questions that may be configured and updated from time to time, Mindshare owns all rights to the intellectual property and material contained in this Site, and all such rights are reserved. Payments submitted to Mindshare is for Hosting and Use of the Mindshare Commercial Off the Shelf Software and Services; which includes configurations tailored for specific uses that are within the defined parameters of the service and that all aspects of the Host Service, including but not limited to the source code, dashboards, analytics and data science are proprietary and remain the sole property of Mindshare.

Mindshare Consulting Group, TACF, ADXL, ICARE, CPRS and Visibility Grid are trademarks of Mindshare Consulting Group. All other product and brand names may be trademarks or registered trademarks of their respective owners.

If you disagree with any of the above statements, please contact the system administrator before accessing this site.

EXHIBIT B

New Hampshire Department of Health and Human Services



DHHS INFORMATION SECURITY REQUIREMENTS

Confidential Information: For the purpose of this Agreement, the Department's Confidential information includes any and all information owned or managed by the State of NH - created, received from or on behalf of the Department of Health and Human Services (DHHS) or accessed in the course of performing contracted services - of which collection, development, protection and disposition is governed by state or federal law or regulation. This information includes, but is not limited to Personal Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI), Social Security Numbers (SSN), Payment Card Industry (PCI) and/or other sensitive and confidential information.

2. The vendor will maintain proper security controls to protect Department confidential information collected, processed, managed, and/or stored in the delivery of contracted services. Minimum expectations include:
 - 2.1 Maintain policies and procedures to protect Department confidential information throughout the information lifecycle, where applicable (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e. tape, disk, paper, etc.)
 - 2.2 Maintain appropriate authentication and access controls to contractor systems that collect, transmit, or store Department confidential information where applicable.
 - 2.3 Encrypt, at a minimum, any Department confidential data stored on portable media, e.g. laptops, USB drives, as well as when transmitted over public networks like the Internet using current industry standards and best practices for strong encryption.
 - 2.4 Ensure proper security monitoring capabilities are in place to detect potential security events that can impact State of NH systems and/or Department confidential information for contractor provided systems.
 - 2.5 Provide security awareness and education for its employees, contractors and sub-contractors in support of protecting Department confidential information.
 - 2.6. Maintain a documented breach notification and incident response process. The vendor will contact the Department within twenty-four (24) hours to the Department's contract manager, and additional email addresses provided in this section, of a confidential information breach, computer security incident, or suspected breach which affects or includes any State of New Hampshire systems that connect to the State of New Hampshire network.
 - 2.6.1 "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45: Code of Federal Regulations. "Computer Security Incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce. Breach notifications will be sent to the following email addresses:
 - 2.6.1.1 Chris.Chen@computer.offices@state.nh.gov
 - 2.6.1.2 DHHSInformationSecurity@ksb.state.nh.gov
- 2.7 If the vendor will maintain any Confidential Information on its systems (or its sub-contractor systems), the vendor will maintain a documented process for securely disposing of such data upon request or contract termination, and will obtain written certification for any State of New Hampshire data destroyed by the vendor or any subcontractors as a part of ongoing, emergency, and/or disaster recovery operations. When no longer in use, electronic media containing State of New Hampshire data shall be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing). The vendor will

Contract number _____

Page 1-12

Date _____

New Hampshire Department of Health and Human Services



document and certify in writing at time of the data destruction, and will provide written certification to the Department upon request. The written certification will include all details necessary to demonstrate data has been properly destroyed and validated. Where applicable, regulatory and professional standards for retention requirements will be jointly evaluated by the State and vendor prior to destruction.

- 2.8 If the vendor will be sub-contracting any core functions of the engagement supporting the services for State of New Hampshire, the vendor will maintain a program of an internal process or processes that defines specific security expectations and monitoring compliance to security requirements that at a minimum match those for the vendor, including breach notification requirements.
- 3 The vendor will work with the Department to sign and comply with all applicable State of New Hampshire and Department system access and authorization policies and procedures, systems access forms, and computer use agreements as part of obtaining and maintaining access to any Department system(s). Agreements will be completed and signed by the vendor and any applicable sub-contractors prior to system access being authorized.
- 4 If the Department determines the vendor is a Business Associate pursuant to 45 CFR 160.103, the vendor will work with the Department to sign and execute a HIPAA Business Associate Agreement (BAA) with the Department and is responsible for maintaining compliance with the agreement.
- 5 The vendor will work with the Department at its request to complete a survey. The purpose of the survey is to enable the Department and vendor to monitor for any changes in risks, threats, and vulnerabilities that may occur over the life of the vendor engagement. The survey will be completed annually or an alternate time frame at the Department's discretion with agreement by the vendor, or the Department may request the survey be completed when the scope of the engagement between the Department and the vendor changes. The vendor will not store knowingly or unknowingly any State of New Hampshire or Department data offshore or outside the boundaries of the United States unless prior express written consent is obtained from the appropriate authorized data owner or leadership member within the Department.

EXHIBIT C

Health Insurance Portability and Accountability Act Business Associate Agreement

Eckerd Youth Alternatives, Inc. d/b/a Eckerd Kids ("Eckerd Kids") and Mindshare Consulting Group, LLC ("Mindshare") agree to comply with the Health Insurance Portability and Accountability Act, Public Law 104-191 and with the Standards for Privacy and Security of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 and those parts of the HITECH Act applicable to business associates. As defined herein, "Business Associate" shall mean Eckerd Kids and Mindshare and any of their subcontractors or agents that receive, use or have access to protected health information under this Agreement and "Covered Entity" shall mean the Department of Health and Human Services.

(1) Definitions

- a. "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45 Code of Federal Regulations
- b. "Breach Notification Rule" shall mean the provisions of the Notification in the Case of Breach of Unsecured Protected Health Information at 45 CFR Part 164, Subpart D and amendments thereto
- c. "Business Associate" has the meaning given such term in section 160.103 of Title 45 Code of Federal Regulations
- d. "Covered Entity" has the meaning given such term in section 160.103 of Title 45, Code of Federal Regulations
- e. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR Section 164.501
- f. "Data Aggregation" shall have the same meaning as the term "data aggregation" in 45 CFR Section 164.501
- g. "Health Care Operations" shall have the same meaning as the term "health care operations" in 45 CFR Section 164.501
- h. "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D Part 1 & 2 of the American Recovery and Reinvestment Act of 2009.
- i. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 and the Standards for Privacy and Security of Individually Identifiable Health Information 45 CFR Parts 160, 162 and 164.
- j. "Individual" shall have the same meaning as the term "individual" in 45 CFR Section 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR Section 164.502(g)

- k. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164 promulgated under HIPAA by the United States Department of Health and Human Services
- l. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR Section 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
- m. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR Section 164.103.
- n. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- o. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C, and amendments thereto.
- p. "Unsecured Protected Health Information" shall have the same meaning given such term in section 164.402 of Title 45, Code of Federal Regulations
- q. Other Definitions - All terms not otherwise defined herein shall have the meaning established under 45 C.F.R. Parts 160, 162 and 164 as amended from time to time, and the HITECH Act

(2) Use and Disclosure of Protected Health Information.

- a. Business Associate shall not use, disclose, maintain or transmit Protected Health Information (PHI) except as reasonably necessary to provide the services outlined under the Agreement. Further, the Business Associate, and its directors, officers, employees and agents, shall not use, disclose, maintain or transmit PHI in any manner that would constitute a violation of the Privacy and Security Rule.
- b. Business Associate may use or disclose PHI
 - I. For the proper management and administration of the Business Associate,
 - II. As required by law pursuant to the terms set forth in paragraph d below, or
 - III. For data aggregation purposes for the health care operations of Covered Entity.
- c. To the extent Business Associate is permitted under the Agreement (including this Exhibit) to disclose PHI to a third party, Business Associate must obtain prior to making any such disclosure, (i) reasonable assurances from the third party that such PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the third party, and (ii) an agreement from such third party to notify Business Associate, in accordance with 45 CFR 164.410, of any breaches of the confidentiality of the PHI to the extent it has obtained knowledge of such breach
- d. The Business Associate shall not disclose any PHI in response to a request for disclosure on the basis that it is required by law without first notifying Covered Entity so that Covered Entity has an opportunity to object to the disclosure and to seek appropriate relief. If Covered Entity objects to such disclosure the Business Associate

shall refrain from disclosing the PHI until Covered Entity has exhausted all remedies. If Covered Entity does not object to such disclosure within five (5) business days of Business Associate's notification, then Business Associate may choose to disclose this information or object as Business Associate deems appropriate.

- e. If the Covered Entity notifies the Business Associate that Covered Entity has agreed to be bound by additional restrictions over and above those uses or disclosures or security safeguards of PHI pursuant to the Privacy and Security Rule, the Business Associate shall be bound by such additional restrictions and shall not disclose PHI in violation of such additional restrictions and shall abide by any additional reasonable security safeguards.

(3) Obligations and Activities of Business Associate

- a. The Business Associate shall notify the Covered Entity's Privacy Officer without unreasonable delay and in no case later than two (2) business days following the date upon which the Business Associate becomes aware of any use or disclosure of protected health information not provided for by the Agreement or this Exhibit, including breaches of unsecured protected health information and/or any security incident that may have an impact on the protected health information of the Covered Entity.

- b. The Business Associate shall promptly perform a risk assessment when it becomes aware of any of the above situations. The risk assessment shall include, but not be limited to, the following information, to the extent it is known by the Business Associate:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

The Business Associate shall complete the risk assessment without unreasonable delay and in no case later than two (2) business days of discovery of the breach and after completion, immediately report the findings of the risk assessment in writing to the Covered Entity.

- c. The Business Associate shall comply with all applicable sections of the Privacy, Security, and Breach Notification Rule.
- d. Business Associate shall make available all of its internal policies and procedures, books and records relating to the use and disclosure of PHI received from or created or received by the Business Associate on behalf of Covered Entity to the Secretary for purposes of determining Covered Entity's compliance with HIPAA and the Privacy and Security Rule.
- e. Business Associate shall require all of its business associates that receive, use or have access to PHI under the Agreement to agree in writing to adhere to the same restrictions and conditions on the use and disclosure of PHI contained herein, including the duty to return or destroy the PHI as provided under Section 3(l) herein. The Covered Entity shall be considered a direct third party beneficiary of the Contractor's business associate agreements with Contractor's intended business associates who will be receiving PHI.

pursuant to this Agreement, with rights of enforcement and indemnification from such business associates who shall be governed by the Agreement for the purpose of use and disclosure of protected health information

- f. Within five (5) business days of receipt of a written request from Covered Entity, Business Associate shall make available during normal business hours at its offices all records, books, agreements, policies and procedures relating to the use and disclosure of PHI to the Covered Entity, for purposes of enabling Covered Entity to determine Business Associate's compliance with the terms of this Exhibit.
- g. Within ten (10) business days of receiving a written request from Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set to the Covered Entity, or as directed by Covered Entity, to an individual in order to meet the requirements under 45 CFR Section 164.524
- n. Within ten (10) business days of receiving a written request from Covered Entity for an amendment of PHI or a record about an individual contained in a Designated Record Set, the Business Associate shall make such PHI available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under 45 CFR Section 164.528.

Business Associate shall document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR Section 164.528

- . Within ten (10) business days of receiving a written request from Covered Entity for a request for an accounting of disclosures of PHI, Business Associate shall make available to Covered Entity such information as Covered Entity may require to fulfill its obligations to provide an accounting of disclosures with respect to PHI in accordance with 45 CFR Section 164.528
- k. In the event any individual requests access to, amendment of or accounting of PHI directly from the Business Associate the Business Associate shall within two (2) business days forward such request to Covered Entity. Covered Entity shall have the responsibility of responding to forwarded requests. However, if forwarding the individual's request to Covered Entity would cause Covered Entity or the Business Associate to violate HIPAA and the Privacy and Security Rule, the Business Associate shall instead respond to the individual's request as required by such law and notify Covered Entity of such response as soon as practicable.
- l. Within ten (10) business days of termination of the Agreement, for any reason the Business Associate shall return or destroy, as specified by Covered Entity, all PHI received from, or created or received by the Business Associate in connection with the Agreement, and shall not retain any copies or back-up tapes of such PHI. If return or destruction is not feasible, or the disposition of the PHI has been otherwise agreed to in the Agreement, Business Associate shall continue to extend the protections of this Exhibit, to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. If Covered Entity, in its sole discretion, requires that the Business Associate

destroy any or all PHI, the Business Associate shall certify to Covered Entity that the PHI has been destroyed.

(4) Obligations of Covered Entity

- a. Covered Entity shall notify Business Associate of any changes or limitation(s) in its Notice of Privacy Practices provided to individuals in accordance with 45 CFR Section 164.520, to the extent that such change or limitation may affect Business Associate's use or disclosure of PHI.
- b. Covered Entity shall promptly notify Business Associate of any changes in, or revocation of permission provided to Covered Entity by individuals whose PHI may be used or disclosed by Business Associate under this Agreement, pursuant to 45 CFR Section 164.506 or 45 CFR Section 164.508.
- c. Covered entity shall promptly notify Business Associate of any restrictions on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(5) Termination for Cause

The Covered Entity may immediately terminate the Agreement upon Covered Entity's knowledge of a breach by Business Associate of the Business Associate Agreement set forth herein as Exhibit C. The Covered Entity may either immediately terminate the Agreement or provide an opportunity for Business Associate to cure the alleged breach within a timeframe specified by Covered Entity. If Covered Entity determines that neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(6) Miscellaneous

- a. Definitions and Regulatory References. All terms used, but not otherwise defined herein, shall have the same meaning as those terms in the Privacy and Security Rule, and the HITECH Act, as codified at 45 CFR Parts 160 and 164 and as amended from time to time. A reference in the Agreement as amended to include this Exhibit, to a Section in the Privacy and Security Rule means the Section as in effect or as amended.
- b. Amendment. Covered Entity and Business Associate agree to take such action as is necessary to amend the Agreement, including this Exhibit, from time to time as is necessary for Covered Entity to comply with the changes in the requirements of HIPAA, the Privacy and Security Rule, and applicable federal and state law.
- c. Data Ownership. The Business Associate acknowledges that it has no ownership rights with respect to the PHI provided by or created on behalf of Covered Entity under the Agreement.
- d. Interpretation. The parties agree that any ambiguity in the Agreement or this Exhibit shall be resolved to permit Covered Entity to comply with HIPAA, the Privacy and Security Rule and the HITECH Act.